PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-076336

(43)Date of publication of application : 14.03.2000

(51)Int.CI. G06F 17/60
G09C 1/00
H04L 9/32
H04L 12/54
H04L 12/58
H04M 3/42

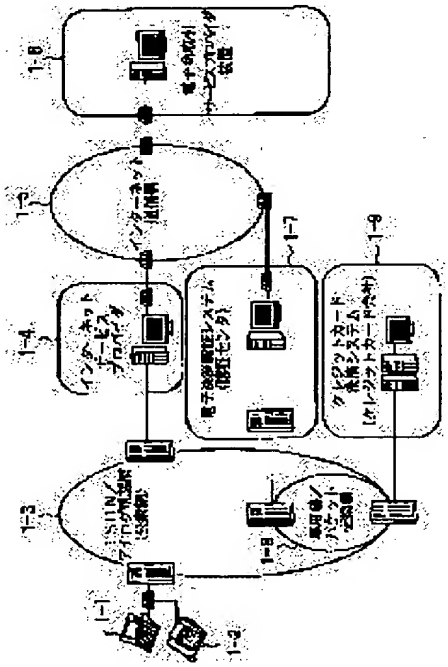
(21)Application number : 10-244726

(22)Date of filing : 31.08.1998

(71)Applicant : FUJITSU LTD

(72)Inventor : FUKUO TARO

(54) ELECTRONIC SETTLEMENT AUTHENTICATION SYSTEM AND ELECTRONIC COMMERCE SERVICE PROVIDER DEVICE



(57)Abstract:

PROBLEM TO BE SOLVED: To easily and securely carry out electronic commerce such as on-line shopping through the Internet by preventing secret information on a credit card number etc., from leaking.

SOLUTION: Order data on an article etc., are sent from a user terminal 1-1 to the electronic commerce service provider device 1-6 through the Internet 1-5 and the electronic commerce provider device sends those data out to an electronic settlement authentication system 1-7. The electronic settlement authentication system calls the user terminal back through a public telephone network 1-3 to receive secret information on a credit card number etc., directly from the user terminal through the public telephone network, sends the secret information to a credit card settlement system 1-9, and receives authentication result data on the credit card number etc., from the credit card settlement system and then sends the authentication result data to the electronic commerce service provider device.

CLAIMS

[Claim(s)]

[Claim 1] Send and receive the data of electronic commerce through the Internet between a user terminal and electronic commerce service provider equipment. In the electronic banking authentication system for the electronic commerce which settles payment of this electronic commerce by the credit card transaction system this electronic banking authentication system If the data of electronic commerce including a user ID child are received from said electronic commerce service provider equipment A means to call back a user terminal through a public network based on this user ID child, and to receive the secrecy information of the user for electronic banking directly through this public network from a user terminal, A means to transmit the secrecy information of the this user who received to a credit card transaction system, and to receive the authentication result data about this user's secrecy information from a credit card transaction system, The electronic banking authentication system characterized by having a means to transmit these authentication result data to said electronic commerce service provider equipment.

[Claim 2] Said electronic banking authentication system is an electronic banking authentication system according to claim 1 characterized by having the configuration which sends and receives information through the public network of said user terminal and ISDN circuit, or an analog telephone line, and sends and receives information data through said credit card transaction system and dedicated line, or a digital data exchange.

[Claim 3] Said electronic banking authentication system is an electronic banking authentication system according to claim 1 or 2 characterized by having the subscriber database storage section which memorizes the subscriber information on the user who registered with this electronic banking authentication system beforehand, and an electronic commerce service provider, and the transaction database storage section which memorizes the order data of the electronic commerce sent and received between a user terminal and electronic commerce service provider equipment.

[Claim 4] They are claim 1 characterized by having the configuration which the subscriber database storage section of said electronic banking authentication system has the configuration which assigns and memorizes the user ID child and electronic commerce service provider identifier of a proper to each user and each electronic commerce service provider, respectively, and said electronic banking authentication system uses those identifiers as a master key, and reads the subscriber information on a user or an electronic commerce service provider from said subscriber database storage section thru/or an electronic banking authentication system given in 3 any 1 terms.

[Claim 5] They are claim 1 which the transaction database storage section of said electronic

banking authentication system has the configuration which assigns and memorizes the transaction identifier of a proper to the order data of each electronic commerce, respectively, and is characterized by equipping said electronic banking authentication system with a means to notify this transaction identifier to said credit card transaction system and said electronic commerce service provider equipment thru/or an electronic banking authentication system given in 4 any 1 terms.

[Claim 6] Said electronic banking authentication system searches this user's telephone number from the subscriber database storage section based on the user ID child transmitted from electronic commerce service provider equipment. A means to call back a user terminal through a public network with this telephone number, Claim 1 characterized by having a means to send out an announcement including the guidance which stimulates transmission of the secrecy information of the user for electronic banking, and the means which carries out reception maintenance of the secrecy information transmitted from the user terminal thru/or an electronic banking authentication system given in 5 any 1 terms.

[Claim 7] Said electronic banking authentication system is equipped with a means to recognize whether the circuit to which the user terminal was connected is an ISDN circuit, or it is an analog telephone line based on the data of said subscriber database storage section. A means to call back said user terminal A user terminal is faced calling back when the circuit to which said user terminal was connected is an ISDN circuit. When the circuit of said user terminal is busy The queuing call or call waiting call which waits for and calls busy termination is performed. The electronic banking authentication system according to claim 6 characterized by having the configuration which performs the queuing call or call waiting call which waits for and calls termination of the Internet connectivity of said user terminal when the circuit to which said user terminal was connected is an analog telephone line.

[Claim 8] A means to provide a user terminal with the display screen for electronic commerce through the Internet, and to receive the order data of electronic commerce with a user ID child from a user terminal, A means to transmit this user ID child and the order data of electronic commerce to an electronic banking authentication system through the Internet, A means to receive said user ID child and the authentication result information about said electronic commerce from said electronic banking authentication system, Electronic commerce service provider equipment characterized by having a means to transmit this authentication result information to said user terminal with the transaction identifier of the order data of said electronic commerce.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the electronic banking authentication system

and electronic commerce service provider equipments in electronic commerce, such as on-line shopping by the Internet.

[0002] The commercial on line service by the Internet spreads in recent years, and the opportunity for the individual secrecy information for electronic banking to be transmitted and received on the Internet is increasing. The individual secrecy information sent and received for electronic banking is protected by insurance, and construction of the system which can perform quick and simple electronic banking is demanded as use of the electronic commerce by such commercial on line service increases.

[0003] In on-line shopping, virtual Mall shopping, etc. by the Internet for a user side It is the system by which the secrecy information which secrecy information, such as a credit card number, was transmitted to insurance, and was transmitted is not abused by revealing, moreover, for an electronic commerce service provider side It is important that the user who accessed electronic commerce service is him of Shinsei of a commercial transaction, and it is the system by which the corroboration of the price using the credit card number information transmitted by the user that there is no trouble in paying is obtained.

[0004]

[Description of the Prior Art] In case the electronic commerce service by the Internet is used, transmission of secrecy information, such as a credit card number, is required of a user in many cases at the time of the purchase of goods etc. Although the encoding technology and the secret communication technique of transmit data are used in transmission of secrecy information, in the present condition, the safety to secrecy information can never say that it is enough only with those techniques.

[0005] Because, since the information dispatch in the Internet goes via many and unspecified servers in which a management engine is not necessarily clear, it has a possibility that the surreptitious use improper use of the secrecy information may be carried out. Therefore, the following policies were conventionally taken about the treatment of secrecy information, such as a credit card number, for example.

[0006] One of them is the approach of transmitting the order data and the user name of electronic commerce, and performing electronic commerce, without transmitting to each electronic commerce service provider side by the Internet and other means of communications, and the user's registering secrecy information, such as a credit card number, beforehand, and transmitting secrecy information, such as a credit card number, to the electronic commerce service utilization time by the Internet.

[0007] However, by this approach, when modification is produced in a credit card number etc., that must be transmitted and notified to each registration place electronic commerce service provider side. Moreover, since secrecy information, such as a credit card number, must be registered, many parts distribute and secrecy information is kept to each electronic commerce service provider side when performing goods purchase etc. from two or more electronic commerce service providers, it is not desirable after that the safety to a nondisclosure

manages.

[0008] As other approaches, the method of transmitting secrecy information, such as a credit card number, to an electronic commerce service provider side with a facsimile image is in the electronic commerce service utilization time by the Internet. However, by this approach, the document with which the credit card number was written down is outputted to the facsimile apparatus by the side of an electronic commerce service provider, and if that storage management is unsuitable, since hard copy etc. can be performed easily, a possibility that secrecy information may be used unjustly will arise.

[0009]

[Problem(s) to be Solved by the Invention] In electronic commerce, such as online SHOPINGU service by the Internet, a user transmits and purchases a credit card number etc. to finish settlement of goods price simple. However, the cure of security was not thoroughgoing to transmission of the secrecy information which went via the Internet, and the check of the electronic commerce data to trouble generating of the unjust claim by the multiplex claim by the procedure mistake by the side of an electronic commerce service provider, other users' wrongful act, etc. had become it with the complicated thing in the electronic commerce service by the Internet.

[0010] Furthermore, when a user used the electronic commerce service provider from which plurality differs, conventionally, the electronic commerce service from the electronic commerce service provider which it is necessary to register information, such as a credit card number, for every electronic commerce service provider, and unitary management of secrecy information cannot be performed, and has not registered credit card number information etc. in advance could not be used, but was inconvenience.

[0011] This invention aims at simple and offering the electronic banking authentication system which can perform electronic commerce, and electronic commerce service provider equipment safely in the electronic commerce service by the Internet, without preventing leakage of secrecy information, such as a credit card number, and being able to perform maintenance and a check of electronic commerce data, and the user registering secrecy information, such as a credit card number, beforehand.

[0012]

[Means for Solving the Problem] The electronic banking authentication system of this invention sends and receives the data of electronic commerce through the Internet between (1) user terminal and electronic commerce service provider equipment. In the electronic banking authentication system for the electronic commerce which settles payment of this electronic commerce by the credit card transaction system this electronic banking authentication system If the data of electronic commerce including a user ID child are received from said electronic commerce service provider equipment A means to call back a user terminal through a public network based on this user ID child, and to receive the secrecy information of the user for electronic banking directly through this public network from a

user terminal, A means to transmit the secrecy information of the this user who received to a credit card transaction system, and to receive the authentication result data about this user's secrecy information from a credit card transaction system, It has a means to transmit these authentication result data to said electronic commerce service provider equipment.

[0013] (2) -- said electronic banking authentication system is equipped with the configuration which sends and receives information through the public network of said user terminal and ISDN circuit, or an analog telephone line, and sends and receives information data through said credit card transaction system and dedicated line, or a digital data exchange. [moreover,]

[0014] (3) -- said electronic banking authentication system is equipped with the subscriber database storage section which memorizes the subscriber information on the user who registered with this electronic banking authentication system beforehand, and an electronic commerce service provider, and the transaction database storage section which memorizes the order data of the electronic commerce sent and received between a user terminal and electronic commerce service provider equipment. [moreover,]

[0015] (4) -- the subscriber database storage section of said electronic banking authentication system has the configuration which assigns and memorizes the user ID child and electronic commerce service provider identifier of a proper to each user and each electronic commerce service provider, respectively, and said electronic banking authentication system has the configuration which reads the subscriber information on a user or an electronic commerce service provider from said subscriber database storage section by using those identifiers as a master key. [moreover,]

[0016] (5) -- the transaction database storage section of said electronic banking authentication system has the configuration which assigns and memorizes the transaction identifier of a proper to the order data of each electronic commerce, respectively, and said electronic banking authentication system is equipped with a means to notify this transaction identifier to said credit card transaction system and said electronic commerce service provider equipment. [moreover,]

[0017] (6) -- said electronic-banking authentication system searches this user's telephone number from the subscriber database storage section based on the user-ID child transmitted from electronic-commerce service provider equipment, and is equipped with a means send out an announcement including a means call back a user through a public network with this telephone number, and the guidance which stimulates transmission of the secrecy information of a user required for electronic banking, and the means which carry out the reception maintenance of the secrecy information transmitted from the user terminal. [moreover,]

[0018] Said electronic banking authentication system is equipped with a means to recognize whether the circuit to which the user terminal was connected is an ISDN circuit, or it is an analog telephone line based on the data of said subscriber database storage section. (7) --

[moreover,] A means to call back said user terminal A user terminal is faced calling back when the circuit to which said user terminal was connected is an ISDN circuit. When the circuit of said user terminal is busy The queuing call or call waiting call which waits for and calls busy termination is performed. When the circuit to which said user terminal was connected is an analog telephone line, it has the configuration which performs the queuing call or call waiting call which waits for and calls termination of the Internet connectivity of said user terminal.

[0019] Moreover, the electronic commerce service provider equipment of this invention (8) A means to provide a user terminal with the display screen for electronic commerce through the Internet, and to receive the order data of electronic commerce with a user ID child from a user terminal, A means to transmit this user ID child and the order data of electronic commerce to an electronic banking authentication system through the Internet, It has a means to receive said user ID child and the authentication result information about said electronic commerce from said electronic banking authentication system, and a means to transmit the transaction identifier of the order data of said electronic commerce for this authentication result information to said user terminal.

[0020]

[Embodiment of the Invention] Drawing 1 is the explanatory view of the electronic commerce service system of this invention. this drawing -- setting -- 1-1 -- a user's information-machines-and-equipment terminal and 1-2 -- this user's telephone terminal, and 1-3 -- for the Internet communication network and 1-6, as for an electronic banking authentication system and 1-8, electronic commerce service provider equipment and 1-7 are [ISDN or an analog telephone network, and 1-4 / Internet Service Provider equipment and 1-5 / a dedicated line or a packet exchange network, and 1-9] credit card transaction systems.

[0021] The information-machines-and-equipment terminals 1-1 of user ** are information processors, such as a personal computer, and are connected to ISDN or the analog telephone network 1-3 with this user's telephone terminal 1-2. Here, the information-machines-and-equipment terminal 1-1 and telephone terminal of user ** constitute a user terminal.

[0022] It connects with Internet Service Provider equipment 1-4 through ISDN or the analog telephone network 1-3, and connects with electronic commerce service provider equipment 1-6 via the Internet communication network 1-5, and a user's information-machines-and-equipment terminal 1-1 transmits the data for electronic commerce.

[0023] Electronic commerce service provider equipment 1-6 offers the web page for electronic commerce (homepage) on the Internet, and if the order data for the electronic commerce transmitted by the user are received, it will connect with the electronic banking authentication system 1-7 via the Internet communication network 1-5, and it will carry out the request demand of the authentication at the electronic banking authentication system 1-7

for electronic commerce.

[0024] The electronic banking authentication system 1-7 is equipped with the function to perform authentication for electronic banking alone about a user, to each authentication request demand from two or more electronic commerce service provider equipments 1-6, and functions as an authentication center intensively prepared to two or more electronic commerce service providers.

[0025] The electronic banking authentication system 1-7 calls back a user's telephone terminal 1-2 through ISDN or the analog telephone network 1-3. Secrecy information, such as a credit card number, is received through ISDN or the analog telephone network 1-3 from a user. Moreover, authentication center equipment 1-7 is connected to the credit card transaction system 1-9 through a dedicated line or a packet exchange network 1-8. While notifying the credit card number received from the user to the credit card transaction system 1-9, the inquiry about payment by the credit card number etc. is performed, and it has the function to transmit the result to electronic commerce service provider equipment 1-6.

[0026] The credit card transaction system 1-9 is installed in a credit card company etc., and it checks [which is depended on account draw down etc.] paying for no trouble based on information, such as a credit card number notified from the electronic banking authentication system 1-7, and the amount-of-money information on electronic commerce, and has the function to transmit the result to the electronic banking authentication system 1-7.

[0027] Thus, although transmission and reception of the data through ISDN or the analog telephone network 1-3, the Internet communication network 1-5 and a dedicated line, or a packet exchange network 1-8 perform electronic banking authentication by this invention, the simple Internet communication network 1-5 of actuation is used for transmission and reception of the high information on secrecy nature at transmission and reception of the low information on secrecy nature using ISDN or the analog telephone network 1-3 and a dedicated line, or a packet exchange network 1-8. In addition, the above-mentioned packet exchange network may be a digital data exchange.

[0028] Drawing 2 is drawing showing the principal part of the electronic banking authentication system of this invention. The electronic banking authentication system 2-10 consists of the exchange section 2-3 equipped with the subscriber database storage section 2-1 and the announcement machine 2-2 holding subscriber information, such as a user, and the communication terminal section 2-5 equipped with the transaction database storage section 2-4 in which electronic commerce carries out order data-hold.

[0029] The exchange section 2-3 calls back a user terminal 2-7 through ISDN or the analog telephone network 2-6, sends out the guidance which stimulates sending out of information (a user ID child, credit card number, etc.) required for the claim amount of money and electronic banking with an announcement machine 2-2 by synthesized speech, and has the function to receive information required for electronic banking including secrecy information, such as a credit card number transmitted by the PB signal etc. from the user terminal 2-7.

[0030] Moreover, the exchange section 2-3 has the function which performs a notice and an inquiry to the credit card transaction system 2-9 through a dedicated line or a packet exchange network 2-8, receives the reply result about the received credit card number, and is sent out to the communication terminal section 2-5.

[0031] The communication terminal section 2-5 will transmit to the electronic commerce service provider (CSP) 2-12 through the Internet communication network 2-11, if it connects with the exchange section 2-3 and the reply result from the credit card transaction system 2-9 is received from the exchange section 2-3.

[0032] Thus, it connects with ISDN or the analog telephone network 2-6 and a dedicated line, or a packet exchange network 2-8, and the high information on secrecy nature is sent [the exchange section 2-3] and received through ISDN, the analog telephone network 2-6, a dedicated line, or a packet exchange network 2-8.

[0033] It connects with the Internet communication network 2-11, and the communication terminal section 2-5 sends and receives the low information on secrecy nature through the Internet communication network 2-11. Since the Internet communication link goes via many and unspecified Internet Service Providers, this reason is because it is hard to call it what has the enough safety management to the nondisclosure of communication link information, as it was mentioned above.

[0034] Since it connects with a direct communication partner's transmitter-receiver, information is sent and received and any third persons other than a communications partner do not intervene, there are few dangers that communication link information will flow out, and, as for the communication link which, on the other hand, minded only ISDN which is a public network, the analog telephone network, the packet exchange network, or the dedicated line, whenever [insurance] is high.

[0035] By therefore, the electronic banking authentication system which installed the authentication center where only [which deals with the communication link information as which nondisclosure strict observance is required in electronic commerce service], or a fraction was restricted, and was furnished to this authentication center When it considers as the configuration which carries out the centralized control of the secrecy information unitary and this electronic banking authentication system considers as the configuration which uses a communication network properly according to the secrecy nature of the information sent and received, decentralization and tapping of confidential information can be prevented and the reliable system to confidential information can be built.

[0036] Drawing 3 is the functional block diagram of the electronic banking authentication system of this invention. For CPU of this exchange section, and 3-12, as for the I/O section of the exchange section, and 3-14, in this drawing, the data communication section of the exchange section and 3-13 are [3-1 / the exchange section and 3-11 / the service control section and 3-15] the subscriber database storage sections.

[0037] Moreover, as for 3-2, as for the communication terminal section and 3-21, CPU of this

communication terminal section and 3-22 are the transaction database storage sections in which the data communication section of the communication terminal section, the I/O section of the 3-23 communication-terminal section, and 3-24 hold the WWW (Word Wide Web) database storage section, and 3-25 holds order data.

[0038] The data communication section 3-12 of the exchange section calls back a user's telephone terminal through ISDN or an analog telephone network, receives information, such as a credit card number, and performs a notice and an inquiry to a credit card transaction system through a dedicated line or a packet exchange network about information, such as a received credit card number. It connects with the I/O section 3-23 of the communication terminal section, and mutual, and the I/O section 3-13 of the exchange section has the data communication between the exchange section 3-1 and the communication terminal section 3-2, and a data conversion feature for it.

[0039] It connects with the Internet communication network, and the data communication section 3-22 of the communication terminal section receives the order data of the electronic commerce by the Internet from an electronic commerce service provider, and transmits the inquiry result information from a credit card transaction system etc. to an electronic commerce service provider.

[0040] The subscriber database storage section 3-15 of the exchange section memorizes as a database each user who had the registration demand beforehand, an electronic commerce service provider, and the subscriber information about a credit card company. Therefore, although the user who demands electronic commerce needs to register subscriber information beforehand only to the subscriber database storage section 3-15 of this electronic banking authentication system, in order that it may perform the call-back from an electronic banking authentication system proper, it is the minimum information for managing the transaction data of electronic commerce, and there is no registering-beforehand-secrecy information, such as credit card number, need.

[0041] The WWW database storage section 3-24 of the communication terminal section memorizes the database for the web pages of the Internet, and the transaction database storage section 3-25 holds transaction data, such as order data sent and received between the user and the electronic commerce service provider.

[0042] Drawing 4 is drawing showing the contents of the database storage section of the electronic banking authentication system of this invention. (B of (A) of drawing) of a subscriber database and drawing is a transaction database between a user and an electronic commerce service provider.

[0043] The subscriber database of (A) of drawing memorizes the subscriber information in the form of a chart for every user, electronic commerce service provider, and credit card company. About a user, a user ID child (ID), a name, the address, the telephone number, a service state, etc. are memorized, an electronic commerce service provider identifier (service ID), a firm name, the address, the telephone number, a service state, etc. are memorized about an

electronic commerce service provider, and subscriber information, such as a credit card company identifier (credit ID), a firm name, the other addresses that omitted illustration, the telephone number, and a service state, is memorized about a credit card company.

[0044] furthermore, a subscriber database carries out storage maintenance of each user's circuit class and class of service (for example, an ISDN circuit or an analog telephone line -- moreover -- the subscriber's loop in which call waiting (call waiting) service is possible ****** -- etc. -- data).

[0045] The transaction database of (B) of drawing memorizes a transaction identifier (ID), an authentication result, a credit card company identifier (credit ID), a user ID child (ID), an electronic commerce service provider identifier (service ID), a trade name, the number, a price, etc. in the form of a chart.

[0046] Drawing 5 thru/or drawing 7 are the explanatory views of the communication procedure of electronic commerce service of this invention. As first shown in ** of drawing 5 , by the Internet connectivity, a user transmits the order data about purchase goods, such as user ID, a trade name, and the number, to the database section of the WWW server 5-2 of an electronic commerce service provider (CSP) through an Internet Service Provider (ISP) using the information-machines-and-equipment terminal 5-1.

[0047] Next, as shown in ** of drawing 6 , the WWW server 6-1 of an electronic commerce service provider transmits data, such as Service ID, user ID, a trade name, the number, and a price, to the database section of the electronic banking authentication system 6-2 by the Internet connectivity.

[0048] The electronic banking authentication system 6-2 (it sets to drawing 5 and is 5-3) searches the circuit class and class of service from a subscriber database based on user ID, and a user transmits user ID and a credit card number from the telephone terminal 5-4, as are shown in ** of drawing 5 , and it calls back by public network connection and a user's telephone terminal 5-4 is shown in **' of drawing 5 .

[0049] Here, when a user terminal 5-1 and 5-4 are connected by the ISDN circuit, maintaining connection, since two circuits were used independently without cutting the Internet connectivity circuit of the above-mentioned **, a user can answer with the telephone terminal 5-4 to the call-back from the electronic banking authentication system 5-3 to another circuit, and can receive subsequent authentication service.

[0050] When a user terminal 5-1 and 5-4 are connected by the analog telephone line, a user once cuts the Internet connectivity of the above-mentioned **, and the electronic banking authentication system 5-3 waits for cutting of this Internet connectivity, and performs the queuing call which calls a user's telephone terminal 5-4.

[0051] Although the user of an analog telephone line answers a queuing call from the electronic banking authentication system 5-3 and transmits user ID and a credit card number from the telephone terminal 5-4, the electronic mail through the Internet will receive subsequent authentication service.

[0052] Moreover, when a user terminal 5-1 and the circuit to which 5-4 was connected are ISDN circuits and another circuit mentioned above is busy, the electronic banking authentication system 5-3 waits for cutting of the circuit of the Internet connectivity of the aforementioned **, or another circuit, and performs the queuing call which calls back a user's telephone terminal 5-4.

[0053] In addition, when it is the class of service in which a user can receive a call waiting call (call waiting), the electronic banking authentication system 5-3 can perform a call waiting call instead of the above-mentioned queuing call, it can answer a call-back from the electronic banking authentication system 5-3, maintaining without cutting the Internet connectivity circuit of the above-mentioned **, and can be considered as the configuration which receives subsequent authentication service.

[0054] Next, as shown in ** of drawing 7 , the electronic banking authentication system 7-1 transmits data, such as Transaction ID, user ID, a credit card number, a trade name, and the number, to credit card transaction System 7 -2 through a leased connection or a packet exchange network.

[0055] Credit card transaction System 7 -2 transmits data, such as Service ID, user ID, and an authentication result, to the electronic banking authentication system 7-1 through a leased connection or a packet exchange network, as shown in ** of drawing 7 .

[0056] Next, as shown in ** of drawing 6 , the electronic banking authentication system 6-2 transmits data, such as Transaction ID, user ID, an authentication result, and credit card company ID, to the WWW server 6-1 of an electronic commerce service provider through an Internet connectivity. In addition, you may make it the electronic banking authentication system 6-2 (for it to set to drawing 5 and to be 5-3) announce an authentication result with voice through a public network at this and coincidence to a user's telephone terminal 5-4, as shown at **' of drawing 5 .

[0057] As finally shown in ** of drawing 5 , the detail information and the receipt of order data of electronic commerce are published with Transaction ID through the Internet from the WWW server 5-2 of an electronic commerce service provider. Therefore, a user can check the contents of a detail which include the authentication result of electronic commerce on the screen of a WWW browser immediately.

[0058] Next, the electronic banking authentication system of this invention and the flow of electronic commerce service provider equipment of operation are explained with drawing 8 and drawing 9 . Drawing 8 is the flow chart of actuation of the electronic commerce service provider equipment of this invention. Moreover, drawing 9 is the flow chart of actuation of the electronic banking authentication system of this invention.

[0059] If electronic-commerce service provider equipment will be in the initiation condition of electronic-commerce service of the Internet in step 8-1 shown in drawing 8 , it will display a goods purchase exchange screen by the Web server in step 8-2, and if the basic information input of electronic commerce, such as user ID from a user, the telephone number, and a trade

name of choice, is inputted into waiting and this basic information, it will transmit basic information to an electronic-banking authentication system in step 8-4 in step 8-3.

[0060] If an electronic banking authentication system receives basic information in step 9-1 shown in drawing 9 , in step 9-2, this user ID investigates whether it exists in the subscriber database storage section, if it exists, the telephone number of this user ID will be searched in step 9-3, and if this user's circuit investigates an ISDN circuit or an analog telephone line and it is an ISDN circuit in step 9-4, in step 9-5, it calls back with the registration telephone number.

[0061] Moreover, if a user's circuit is an analog telephone line, the queuing call or call waiting (call waiting) call which waits for and calls busy termination in step 9-6 will be performed. On the other hand, when are called back in the above-mentioned step 9-5 to the user of an ISDN circuit and it is busy (busy), the queuing call or call waiting (call waiting) call which waits for and calls busy termination similarly in step 9-6 is performed.

[0062] If a user's response to a call-back is detected in step 9-7, guidance with voice will be announced in step 9-8, and it will wait for the input of secrecy information, such as a credit card number, in step 9-9. If secrecy information, such as a credit card number, is inputted, in step 9-10, secrecy information and Transactions ID, such as a credit card number, will be transmitted to a credit card transaction system (credit firm), and the authentication result will be received from a credit card transaction system.

[0063] If an authentication result is received from a credit card transaction system, in step 9-11, Transaction ID and the authentication result of a credit card number will be transmitted to electronic commerce service provider equipment. In addition, when user ID does not exist in the above-mentioned step 9-2, the message which refuses the contents of reception in step 9-12 is generated, and the message is transmitted to electronic commerce service provider equipment by step 9-11.

[0064] If electronic commerce service provider equipment receives an authentication result from an electronic banking authentication system, the normality of an authentication result is judged in step 8-5 shown in drawing 8 , and if normal, the screen display of credit card authentication ending [which shows an authentication result to a user terminal in step 8-6], and receipt issue, and the screen of Transaction ID will be displayed, and it will end.

[0065] Moreover, in the judgment of the above-mentioned step 8-5, when an authentication result is abnormal, in step 8-7, the screen for which credit card authentication is improper is displayed, and it returns to the above-mentioned initiation step 8-1 in step 8-8.

[0066] Drawing 10 is the sequence chart of signal transmission and reception of electronic commerce service of this invention. In this drawing, an Internet Service Provider and CSP of the subscriber exchange and ISP in which LS has held the user are electronic commerce service providers.

[0067] The ISDN circuit or analog telephone line which is a public network connects through the subscriber exchange (LS) between a user and an Internet Service Provider (ISP) and

between the authentication centers and users having an electronic banking authentication system.

[0068] The Internet connects between an Internet Service Provider (ISP) and an electronic commerce service provider (CSP), and a dedicated line or a packet exchange network connects between an authentication center and the credit card company equipped with the credit card transaction system.

[0069] A user emits the call to an Internet Service Provider (ISP) at the subscriber exchange (LS) (10-1), a user and an Internet Service Provider (ISP) are connected (10-2), and a user and an electronic commerce service provider (CSP) are connected via this user and an Internet Service Provider (ISP) (10-3).

[0070] A user transmits commercial transaction information, such as user ID and a trade name, to an electronic commerce service provider (CSP) (10-4), and an electronic commerce service provider (CSP) transmits those information to an authentication center (10-5).

[0071] An authentication center investigates a user's telephone number (tele#) with a database from user ID (10-6), and transmits Transaction ID to an electronic commerce service provider (CSP) (10-7).

[0072] Since this transaction ID is transmitted to a user (10-8) and an authentication center calls back the subscriber exchange (LS) in this user, call origination of the electronic commerce service provider (CSP) is carried out (10-9).

[0073] It connects through a public network between an authentication center and a user (10-10), an announcement is sent out so that an authentication center may input secrecy information, such as credit card information, (10-11), and a user inputs secrecy information, such as Transaction ID, user ID, and credit card information, with a telephone terminal (10-12).

[0074] An authentication center registers into a database temporarily the secrecy information inputted by the telephone terminal (10-13), and cuts connection through the public network between users (10-14). An authentication center transmits and asks a credit card company secrecy information, such as credit card information further inputted by the telephone terminal, (10-15), and a credit card company transmits authentication results, such as this credit card information, to an authentication center (10-16).

[0075] An authentication center transmits this authentication result to an electronic commerce service provider (CSP) (10-17), and an electronic commerce service provider (CSP) transmits an attested [credit card] check certificate and a receipt with Transaction ID based on this authentication result (10-18), and a user logs out in response to it, and demands cutting of connection with an Internet Service Provider (ISP) (10-19).

[0076] The subscriber exchange (LS) cuts the connection which minded the public network by the disconnect request from a user (10-20). An electronic commerce service provider (CSP) will ask a credit card company for the goods price by this electronic commerce, and a credit card company will ask a user for the price.

[0077]

[Effect of the Invention] As explained above, according to this invention, secrecy information, such as a credit card number, is directly transmitted only to an electronic banking authentication system through a public network from a user. By carrying out the centralized control of the secrecy information, such as this credit card number, to a credit card transaction system-like the direct question of 1 yuan in all by a dedicated line etc., this electronic banking authentication system Secrecy information, such as credit card information, is not sent and received on the Internet. Since it is not necessary to raise the safety on the management to the outflow of secrecy information etc. and and a user does not need to register credit card information etc. into each electronic commerce service provider beforehand, There is an advantage which can use on-line shopping isoelectronic commercial transaction service immediately by simple actuation.

[0078] in order that [furthermore,] an electronic banking authentication system may perform his identification by calling back an electronic commerce service user based on the subscriber information memorized by the database storage section -- an electronic commerce service provider side and a user side -- him -- the need of the special authentication equipment for identification cannot be carried out, but a simple configuration can perform his identification, and trouble generating of an unjust claim of the tariff by a user's wrongful act etc. can be prevented.

[0079] Since the effectiveness of a user's credit card is notified from an electronic banking authentication system, electronic commerce service provider equipment does not need to perform maintenance of a user's credit card information, and management, and can constitute a system simply.

[0080] By attaching an identifier and managing the transaction data about the electronic commerce exchanged between the user and the electronic commerce service provider in an electronic banking authentication system, a series of commo data of transmission and reception of electronic commerce information and secrecy information can be managed unitary in this electronic banking authentication system, the check at the time of generating of troubles, such as an incorrect claim, can become easy, and electronic commerce service reliability can be raised.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the explanatory view of the electronic commerce service system of this invention.

[Drawing 2] It is drawing showing the principal part of the electronic banking authentication system of this invention.

[Drawing 3] It is the functional block diagram of the electronic banking authentication system

of this invention.

[Drawing 4] It is drawing showing the contents of the database storage section of the electronic banking authentication system of this invention.

[Drawing 5] It is the explanatory view of the communication procedure of electronic commerce service of this invention.

[Drawing 6] It is the explanatory view of the communication procedure of electronic commerce service of this invention.

[Drawing 7] It is the explanatory view of the communication procedure of electronic commerce service of this invention.

[Drawing 8] It is the flow chart of actuation of the electronic commerce service provider equipment of this invention.

[Drawing 9] It is the flow chart of actuation of the electronic banking authentication system of this invention.

[Drawing 10] It is the sequence chart of signal transmission and reception of electronic commerce service of this invention.

[Description of Notations]

1-1 User's Information-Machines-and-Equipment Terminal

1-2 This User's Telephone Terminal

1-3 ISDN or Analog Telephone Network

1-4 Internet Service Provider Equipment

1-5 Internet Communication Network

1-6 Electronic Commerce Service Provider Equipment

1-7 Electronic Banking Authentication System

1-8 Dedicated Line or Packet Exchange Network

1-9 Credit Card Transaction System

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－76336
（P2000－76336A）
(43)公開日　平成12年３月14日(2000.3.14)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｇ０６Ｆ	17/60		Ｃ０６Ｆ	15/21	３４０Ａ
Ｇ０９Ｃ	1/00	６６０	Ｃ０９Ｃ	1/00	６６０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｍ	3/42	Ｚ
	12/54		Ｇ０６Ｆ	15/21	３３０
	12/58		Ｈ０４Ｌ	9/00	６７３Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平10－244726

(22)出願日　平成10年８月31日(1998.8.31)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

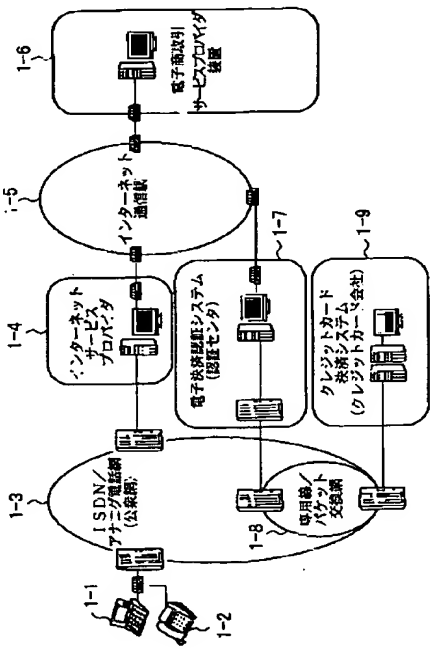
(72)発明者　福生　太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(74)代理人　100072833
弁理士　柏谷　昭司　（外２名）

(54)【発明の名称】　電子決済認証システム及び電子商取引サービスプロバイダ装置

(57)【要約】
【課題】　インターネットによるオンラインショッピング等の電子商取引における電子決済認証システム及び電子商取引サービスプロバイダ装置に関し、クレジットカード番号等の秘匿情報の漏洩を防ぎ、簡便且つ安全に電子商取引を行うことができるようにする。
【解決手段】　ユーザー端末１－１から電子商取引サービスプロバイダ装置１－６にインターネット１－５を介して商品等の注文データを送信し、電子商取引サービスプロバイダ装置はそれらのデータを電子決済認証システム１－７に送出し、電子決済認証システムは公衆網１－３を介してユーザー端末をコールバックし、クレジットカード番号等の秘匿情報をユーザー端末から公衆網を介して直接受信し、秘匿情報をクレジットカード決済システム１－９に送信し、クレジットカード決済システムからクレジットカード番号等の認証結果データを受信し、認証結果データを電子商取引サービスプロバイダ装置に送信する。

本発明の電子商取引サービスシステムの説明図



【特許請求の範囲】
【請求項１】　ユーザー端末と電子商取引サービスプロバイダ装置との間でインターネットを介して電子商取引のデータを送受し、クレジットカード決済システムにより該電子商取引の支払いを決済する電子商取引のための電子決済認証システムにおいて、
該電子決済認証システムは、ユーザー識別子を含む電子商取引のデータを前記電子商取引サービスプロバイダ装置から受信すると、該ユーザー識別子を基に公衆網を介してユーザー端末をコールバックし、電子決済のためのユーザーの秘匿情報をユーザー端末から該公衆網を介して直接受信する手段と、
該受信したユーザーの秘匿情報をクレジットカード決済システムに送信し、クレジットカード決済システムから該ユーザーの秘匿情報についての認証結果データを受信する手段と、
該認証結果データを前記電子商取引サービスプロバイダ装置に送信する手段とを備えたことを特徴とする電子決済認証システム。
【請求項２】　前記電子決済認証システムは、前記ユーザー端末とＩＳＤＮ回線又はアナログ電話回線の公衆網を介して情報を送受し、前記クレジットカード決済システムと専用線又は公衆データ通信網を介して情報データを送受する構成を備えたことを特徴とする請求項１記載の電子決済認証システム。
【請求項３】　前記電子決済認証システムは、該電子決済認証システムに予め登録したユーザー及び電子商取引サービスプロバイダの加入者情報を記憶する加入者データベース記憶部と、ユーザー端末と電子商取引サービスプロバイダ装置との間で送受された電子商取引の注文データを記憶するトランザクションデータベース記憶部とを備えたことを特徴とする請求項１又は２記載の電子決済認証システム。
【請求項４】　前記電子決済認証システムの加入者データベース記憶部は、各ユーザー及び各電子商取引サービスプロバイダに、それぞれ固有のユーザー識別子及び電子商取引サービスプロバイダ識別子を割り付けて記憶する構成を有し、前記電子決済認証システムは、それらの識別子をマスターキーとして前記加入者データベース記憶部より、ユーザー又は電子商取引サービスプロバイダの加入者情報を読み出す構成を有することを特徴とする請求項１乃至３いずれか１項記載の電子決済認証システム。
【請求項５】　前記電子決済認証システムのトランザクションデータベース記憶部は、個々の電子商取引の注文データにそれぞれ固有のトランザクション識別子を割り付けて記憶する構成を有し、前記電子決済認証システムは、該トランザクション識別子を前記クレジットカード決済システム及び前記電子商取引サービスプロバイダ装置に通知する手段を備えたことを特徴とする請求項１乃至４いずれか１項記載の電子決済認証システム。
【請求項６】　前記電子決済認証システムは、電子商取引サービスプロバイダ装置から送信されたユーザー識別子を基に加入者データベース記憶部から該ユーザーの電話番号を検索し、該電話番号により公衆網を介してユーザー端末をコールバックする手段と、電子決済のためのユーザーの秘匿情報の送信を促すガイダンスを含むアナウンスメントを送出する手段と、ユーザー端末から送信された秘匿情報を受信保持する手段とを備えたことを特徴とする請求項１乃至５いずれか１項記載の電子決済認証システム。
【請求項７】　前記電子決済認証システムは、ユーザー端末が接続された回線がＩＳＤＮ回線であるかアナログ電話回線であるかを前記加入者データベース記憶部のデータを基に認識する手段を備え、
前記ユーザー端末をコールバックする手段は、前記ユーザー端末が接続された回線がＩＳＤＮ回線である場合、ユーザー端末をコールバックするに際し、前記ユーザー端末の回線が話中であったときは、話中の終了を待って呼び出す待ち合わせ呼出し又は通話中着信呼び出しを行い、前記ユーザー端末が接続された回線がアナログ電話回線である場合、前記ユーザー端末のインターネット接続の終了を待って呼び出す待ち合わせ呼出し又は通話中着信呼び出しを行う構成を有することを特徴とする請求項６記載の電子決済認証システム。
【請求項８】　ユーザー端末にインターネットを介して電子商取引のための表示画面を提供し、ユーザー端末から電子商取引の注文データをユーザー識別子と共に受信する手段と、
電子決済認証システムにインターネットを介して該ユーザー識別子と電子商取引の注文データとを送信する手段と、
前記電子決済認証システムから前記ユーザー識別子及び前記電子商取引についての認証結果情報を受信する手段と、
前記ユーザー端末へ該認証結果情報を前記電子商取引の注文データのトランザクション識別子とともに送信する手段とを備えたことを特徴とする電子商取引サービスプロバイダ装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、インターネットによるオンラインショッピング等の電子商取引における電子決済認証システム及び電子商取引サービスプロバイダ装置に関する。
【０００２】近年インターネットによる商用オンラインサービスが普及し、電子決済のための個人秘匿情報がインターネット上で送受信される機会が多くなりつつある。このような商用オンラインサービスによる電子商取引の利用が増加するにつれて、電子決済のために送受さ

れる個人秘匿情報が安全に保護され、且つ迅速で簡便な電子決済を行えるシステムの構築が要求されている。

【０００３】インターネットによるオンラインショッピングやバーチャルモールショッピング等において、ユーザー側にとっては、クレジットカード番号等の秘匿情報が安全に送信され、且つ送信した秘匿情報が漏洩して悪用されるようなことがないシステムであること、また、電子商取引サービスプロバイダ側にとっては、電子商取引サービスにアクセスしたユーザーが商取引の真正の本人であり、且つそのユーザーから送信されたクレジットカード番号情報等による代金の支払いに支障がないという確証が得られるシステムであることが重要である。

【０００４】

【従来の技術】インターネットによる電子商取引サービスを利用する際、ユーザーは商品等の購入時にクレジットカード番号等の秘匿情報の送信を要求されることが多い。秘匿情報の送信にあたっては送信データの暗号化技術や秘密通信技術が利用されてはいるが、現状ではそれらの技術のみでは秘匿情報に対する安全性が決して充分であるとはいえない。

【０００５】なぜなら、インターネットにおける情報発信は、必ずしも管理機関の明確でない不特定多数のサーバを経由するため、秘匿情報が盗用悪用されるおそれがある。そのため、従来はクレジットカード番号等の秘匿情報の扱いについて、例えば以下のような方策が取られていた。

【０００６】その一つは、ユーザーはクレジットカード番号等の秘匿情報を、予め各々の電子商取引サービスプロバイダ側へ、インターネット及び他の通信手段により送信して登録しておき、インターネットによる電子商取引サービス利用時にはクレジットカード番号等の秘匿情報を送信することなく、電子商取引の注文データとユーザー名とを送信して電子商取引を行う方法である。

【０００７】しかし、この方法ではクレジットカード番号等に変更を生じた場合、その旨を各登録先電子商取引サービスプロバイダ側へ送信して通知しなければならない。また、複数の電子商取引サービスプロバイダから商品購入等を行う場合、それぞれの電子商取引サービスプロバイダ側へ、クレジットカード番号等の秘匿情報を登録しなければならず、秘匿情報が多数の箇所に分散されて保管されるため、秘密保持に対する安全性の管理の上で好ましくない。

【０００８】他の方法としては、インターネットによる電子商取引サービス利用時に、クレジットカード番号等の秘匿情報をファクシミリ画像により電子商取引サービスプロバイダ側へ送信する方法がある。しかし、この方法では、電子商取引サービスプロバイダ側のファクシミリ装置へクレジットカード番号が書き記された書面が出力され、その保管管理が不適切であったりすると、ハードコピー等が容易に行えることから秘匿情報が不正に使用されるおそれが生じる。

【０００９】

【発明が解決しようとする課題】インターネットによるオンラインショピングサービス等の電子商取引において、簡便に商品代金の決済を済ませたい場合、ユーザーはクレジットカード番号等を送信して購入する。しかし、インターネットを経由した秘匿情報の送信には秘密保護の対策が万全でなく、またインターネットによる電子商取引サービスにおいて、電子商取引サービスプロバイダ側の手続きミスによる多重請求や他のユーザーの不当行為等による不正請求等のトラブル発生に対する電子商取引データの確認作業が煩雑なものとなっていた。

【００１０】更に、ユーザーが複数の異なる電子商取引サービスプロバイダを利用する場合、従来は各電子商取引サービスプロバイダごとにクレジットカード番号等の情報を登録する必要があり、秘匿情報の一元管理ができず、事前にクレジットカード番号情報等を登録していない電子商取引サービスプロバイダからの電子商取引サービスは利用することができず不便であった。

【００１１】本発明は、インターネットによる電子商取引サービスにおいて、クレジットカード番号等の秘匿情報の漏洩を防ぎ、電子商取引データの保持・確認が行え、またユーザーが予めクレジットカード番号等の秘匿情報を登録しておくことなく簡便且つ安全に電子商取引を行うことができる電子決済認証システム及び電子商取引サービスプロバイダ装置を提供することを目的とする。

【００１２】

【課題を解決するための手段】本発明の電子決済認証システムは、（１）ユーザー端末と電子商取引サービスプロバイダ装置との間でインターネットを介して電子商取引のデータを送受し、クレジットカード決済システムにより該電子商取引の支払いを決済する電子商取引のための電子決済認証システムにおいて、該電子決済認証システムは、ユーザー識別子を含む電子商取引のデータを前記電子商取引サービスプロバイダ装置から受信すると、該ユーザー識別子を基に公衆網を介してユーザー端末をコールバックし、電子決済のためのユーザーの秘匿情報をユーザー端末から該公衆網を介して直接受信する手段と、該受信したユーザーの秘匿情報をクレジットカード決済システムに送信し、クレジットカード決済システムから該ユーザーの秘匿情報についての認証結果データを受信する手段と、該認証結果データを前記電子商取引サービスプロバイダ装置に送信する手段とを備えたものである。

【００１３】また（２）前記電子決済認証システムは、前記ユーザー端末とＩＳＤＮ回線又はアナログ電話回線の公衆網を介して情報を送受し、前記クレジットカード決済システムと専用線又は公衆データ通信網を介して情報データを送受する構成を備えたものである。

【００１４】また（３）前記電子決済認証システムは、該電子決済認証システムに予め登録したユーザー及び電子商取引サービスプロバイダの加入者情報を記憶する加入者データベース記憶部と、ユーザー端末と電子商取引サービスプロバイダ装置との間で送受された電子商取引の注文データを記憶するトランザクションデータベース記憶部とを備えたものである。

【００１５】また（４）前記電子決済認証システムの加入者データベース記憶部は、各ユーザー及び各電子商取引サービスプロバイダに、それぞれ固有のユーザー識別子及び電子商取引サービスプロバイダ識別子を割り付けて記憶する構成を有し、前記電子決済認証システムは、それらの識別子をマスターキーとして前記加入者データベース記憶部より、ユーザー又は電子商取引サービスプロバイダの加入者情報を読み出す構成を有するものである。

【００１６】また（５）前記電子決済認証システムのトランザクションデータベース記憶部は、個々の電子商取引の注文データにそれぞれ固有のトランザクション識別子を割り付けて記憶する構成を有し、前記電子決済認証システムは、該トランザクション識別子を前記クレジットカード決済システム及び前記電子商取引サービスプロバイダ装置に通知する手段を備えたものである。

【００１７】また（６）前記電子決済認証システムは、電子商取引サービスプロバイダ装置から送信されたユーザー識別子を基に加入者データベース記憶部から該ユーザーの電話番号を検索し、該電話番号により公衆網を介してユーザーをコールバックする手段と、電子決済に必要なユーザーの秘匿情報の送信を促すガイダンスを含むアナウンスメントを送出する手段と、ユーザー端末から送信された秘匿情報を受信保持する手段とを備えたものである。

【００１８】また（７）前記電子決済認証システムは、ユーザー端末が接続された回線がＩＳＤＮ回線であるかアナログ電話回線であるかを前記加入者データベース記憶部のデータを基に認識する手段を備え、前記ユーザー端末をコールバックする手段は、前記ユーザー端末が接続された回線がＩＳＤＮ回線である場合、ユーザー端末をコールバックするに際し、前記ユーザー端末の回線が話中であったときは、話中の終了を待って呼び出す待ち合わせ呼出し又は通話中着信呼び出しを行い、前記ユーザー端末が接続された回線がアナログ電話回線である場合、前記ユーザー端末のインターネット接続の終了を待って呼び出す待ち合わせ呼出し又は通話中着信呼び出しを行う構成を有するものである。

【００１９】また本発明の電子商取引サービスプロバイダ装置は、（８）ユーザー端末にインターネットを介して電子商取引のための表示画面を提供し、ユーザー端末から電子商取引の注文データをユーザー識別子と共に受信する手段と、電子決済認証システムにインターネットを介して該ユーザー識別子と電子商取引の注文データとを送信する手段と、前記電子決済認証システムから前記ユーザー識別子及び前記電子商取引についての認証結果情報を受信する手段と、前記ユーザー端末へ該認証結果情報を前記電子商取引の注文データのトランザクション識別子とともにを送信する手段とを備えたものである。

【００２０】

【発明の実施の形態】図１は本発明の電子商取引サービスシステムの説明図である。同図において、１－１はユーザーの情報機器端末、１－２は同ユーザーの電話端末、１－３はＩＳＤＮ又はアナログ電話網、１－４はインターネットサービスプロバイダ装置、１－５はインターネット通信網、１－６は電子商取引サービスプロバイダ装置、１－７は電子決済認証システム、１－８は専用線又はパケット交換網、１－９はクレジットカード決済システムである。

【００２１】ユーザー宅の情報機器端末１－１はパーソナルコンピュータ等の情報処理装置であり、同ユーザーの電話端末１－２とともにＩＳＤＮ又はアナログ電話網１－３に接続される。ここで、ユーザー宅の情報機器端末１－１及び電話端末によりユーザー端末を構成する。

【００２２】ユーザーの情報機器端末１－１はＩＳＤＮ又はアナログ電話網１－３を介してインターネットサービスプロバイダ装置１－４に接続され、インターネット通信網１－５を経由して電子商取引サービスプロバイダ装置１－６に接続し、電子商取引のためのデータを送信する。

【００２３】電子商取引サービスプロバイダ装置１－６は、インターネット上で電子商取引のためのウェブページ（ホームページ）を提供し、ユーザーから送信された電子商取引のための注文データを受信すると、インターネット通信網１－５を経由して電子決済認証システム１－７に接続し、電子商取引のため認証を電子決済認証システム１－７に依頼要求する。

【００２４】電子決済認証システム１－７は、複数の電子商取引サービスプロバイダ装置１－６からの各認証依頼要求に対して、ユーザーについて電子決済のための認証を一手に行う機能を備え、複数の電子商取引サービスプロバイダに対して集中的に設けられる認証センタとして機能する。

【００２５】電子決済認証システム１－７は、ＩＳＤＮ又はアナログ電話網１－３を介してユーザーの電話端末１－２をコールバックし、クレジットカード番号等の秘匿情報をユーザーからＩＳＤＮ又はアナログ電話網１－３を介して受信し、また、認証センタ装置１－７は専用線又はパケット交換網１－８を介してクレジットカード決済システム１－９に接続し、ユーザーから受信したクレジットカード番号等をクレジットカード決済システム１－９に通知するとともにそのクレジットカード番号等による支払いについての問い合わせを行い、その結果を

電子商取引サービスプロバイダ装置１－６に送信する機能を有している。

【００２６】クレジットカード決済システム１－９は、クレジットカード会社等に設置され、電子決済認証システム１－７から通知されたクレジットカード番号等の情報と電子商取引の金額情報とを基に、口座引落等による支払いに支障がないかをチェックし、その結果を電子決済認証システム１－７に送信する機能を有する。

【００２７】このように本発明による電子決済認証は、ＩＳＤＮ又はアナログ電話網１－３、インターネット通信網１－５及び専用線又はパケット交換網１－８を介したデータの送受により行うが、このうち、秘匿性の高い情報の送受にはＩＳＤＮ又はアナログ電話網１－３及び専用線又はパケット交換網１－８を用い、秘匿性の低い情報の送受には操作の簡便なインターネット通信網１－５を用いるようにしたものである。なお、前述のパケット交換網は公衆データ通信網であってもよい。

【００２８】図２は本発明の電子決済認証システムの主要部を示す図である。電子決済認証システム２－１０は、ユーザー等の加入者情報を保持する加入者データベース記憶部２－１及びアナウンスメントマシン２－２を備えた交換機部２－３と、電子商取引の注文データ保持するトランザクションデータベース記憶部２－４を備えた通信端末部２－５とから構成される。

【００２９】交換機部２－３はＩＳＤＮ又はアナログ電話網２－６を介してユーザー端末２－７をコールバックし、アナウンスメントマシン２－２により請求金額及び電子決済に必要な情報（ユーザー識別子、クレジットカード番号等）の送出を促すガイダンスを合成音声により送出し、ユーザー端末２－７からＰＢ信号等により送信されたクレジットカード番号等の秘匿情報を含む電子決済に必要な情報を受信する機能を有する。

【００３０】また、交換機部２－３は受信したクレジットカード番号等に関して、専用線又はパケット交換網２－８を介してクレジットカード決済システム２－９に通知及び問い合わせを行い、その回答結果を受信して通信端末部２－５に送出する機能を有する。

【００３１】通信端末部２－５は、交換機部２－３と接続され、クレジットカード決済システム２－９からの回答結果を交換機部２－３から受信すると、インターネット通信網２－１１を介して電子商取引サービスプロバイダ（ＣＳＰ）２－１２に送信する。

【００３２】このように、交換機部２－３はＩＳＤＮ又はアナログ電話網２－６及び専用線又はパケット交換網２－８へ接続され、秘匿性の高い情報をＩＳＤＮ若しくはアナログ電話網２－６又は専用線若しくはパケット交換網２－８を介して送受する。

【００３３】通信端末部２－５は、インターネット通信網２－１１へ接続され、秘匿性の低い情報はインターネット通信網２－１１を介して送受する。この理由は、前述したとおりインターネット通信は不特定多数のインターネットサービスプロバイダを経由するため、通信情報の秘密保持に対する安全管理が充分なものとはいい難いためである。

【００３４】一方、公衆網であるＩＳＤＮ、アナログ電話網、パケット交換網又は専用線のみを介した通信は、直接通信相手の送受信装置と接続されて情報が送受され、通信相手以外の第三者が介在することがないので、通信情報が流出する危険性が少なく安全度が高い。

【００３５】したがって、電子商取引サービスにおいて、秘密保持厳守が要求される通信情報を取り扱う唯一又は少数の限られた認証センタを設置し、該認証センタに設備された電子決済認証システムにより、秘匿情報を一元的に集中管理する構成とし、且つ、該電子決済認証システムは、送受する情報の秘匿性に応じて通信網を使い分ける構成とすることにより、秘密情報の分散化と盗聴を防ぎ、秘密情報に対する信頼性の高いシステムを構築することができる。

【００３６】図３は本発明の電子決済認証システムの機能ブロック図である。同図において、３－１は交換機部、３－１１は該交換機部のＣＰＵ、３－１２は交換機部のデータ通信部、３－１３は交換機部の入出力部、３－１４はサービス制御部、３－１５は加入者データベース記憶部である。

【００３７】また、３－２は通信端末部、３－２１は該通信端末部のＣＰＵ、３－２２は通信端末部のデータ通信部、３－２３通信端末部の入出力部、３－２４はＷＷＷ（Ｗｏｒｄ　Ｗｉｄｅ　Ｗｅｂ）データベース記憶部、３－２５は注文データを保持するトランザクションデータベース記憶部である。

【００３８】交換機部のデータ通信部３－１２は、ＩＳＤＮ又はアナログ電話網を介してユーザーの電話端末をコールバックし、クレジットカード番号等の情報を受信し、受信したクレジットカード番号等の情報について専用線又はパケット交換網を介してクレジットカード決済システムに通知及び問い合わせを行う。交換機部の入出力部３－１３は、通信端末部の入出力部３－２３と相互に接続され、交換機部３－１と通信端末部３－２との間のデータ通信及びそのためのデータ変換機能を有する。

【００３９】通信端末部のデータ通信部３－２２はインターネット通信網に接続され、電子商取引サービスプロバイダからインターネットによる電子商取引の注文データを受信し、また電子商取引サービスプロバイダにクレジットカード決済システムからの問い合わせ結果情報等を送信する。

【００４０】交換機部の加入者データベース記憶部３－１５は、予め登録要求のあった各ユーザー、電子商取引サービスプロバイダ及びクレジットカード会社についての加入者情報をデータベースとして記憶する。したがって、電子商取引を要望するユーザーは、この電子決済認

証システムの加入者データベース記憶部３－１５に対してのみ加入者情報を予め登録しておく必要があるが、それは電子決済認証システムからのコールバックを適正に行うためと、電子商取引のトランザクションデータを管理するための最少限の情報であり、クレジットカード番号等の秘匿情報を予め登録しておくこと必要はない。

【００４１】通信端末部のWWWデータベース記憶部３－２４は、インターネットのウェブページ用のデータベースを記憶し、またトランザクションデータベース記憶部３－２５は、ユーザーと電子商取引サービスプロバイダとの間で送受された注文データ等のトランザクションデータを保持する。

【００４２】図４は本発明の電子決済認証システムのデータベース記憶部の内容を示す図である。図の（Ａ）は加入者データベース、図の（Ｂ）はユーザーと電子商取引サービスプロバイダとの間のトランザクションデータベースである。

【００４３】図の（Ａ）の加入者データベースは、各ユーザー、電子商取引サービスプロバイダ及びクレジットカード会社ごとに、その加入者情報を一覧表の形式で記憶したものである。ユーザーについては、ユーザー識別子（ＩＤ）、氏名、住所、電話番号、サービス状態等が記憶され、電子商取引サービスプロバイダについては、電子商取引サービスプロバイダ識別子（サービスＩＤ）、会社名、住所、電話番号、サービス状態等が記憶され、クレジットカード会社については、クレジットカード会社識別子（クレジットＩＤ）、会社名、その他図示を省略した住所、電話番号、サービス状態等の加入者情報を記憶する。

【００４４】更に、加入者データベースは、各ユーザーの回線種別及びサービスクラス（例えば、ＩＳＤＮ回線かアナログ電話回線か、又通話中着信（コールウェイティング）サービスが可能な加入者回線か否か等のデータ）を記憶保持する。

【００４５】図の（Ｂ）のトランザクションデータベースは、トランザクション識別子（ＩＤ）、認証結果、クレジットカード会社識別子（クレジットＩＤ）、ユーザー識別子（ＩＤ）、電子商取引サービスプロバイダ識別子（サービスＩＤ）、商品名、個数、価格等を一覧表の形式で記憶する。

【００４６】図５乃至図７は本発明の電子商取引サービスの通信手順の説明図である。先ず図５の① に示すようにユーザーは情報機器端末５－１を用いてインターネット接続により、ユーザーＩＤ、商品名、個数等の購入商品に関する注文データを、インターネットサービスプロバイダ（ＩＳＰ）を介し、電子商取引サービスプロバイダ（ＣＳＰ）のWWWサーバー５－２のデータベース部に送信する。

【００４７】次に図６の② に示すように電子商取引サービスプロバイダのWWWサーバー６－１は、サービスＩＤ、ユーザーＩＤ、商品名、個数、価格等のデータを、インターネット接続により電子決済認証システム６－２のデータベース部に送信する。

【００４８】電子決済認証システム６－２（図５においては５－３）は、ユーザーＩＤを基に加入者データベースからその回線種別及びサービスクラスを検索し、図５の③ に示すようにユーザーの電話端末５－４を公衆網接続によりコールバックし、ユーザーは図５の③′ に示すように電話端末５－４からユーザーＩＤとクレジットカード番号を送信する。

【００４９】ここで、ユーザー端末５－１，５－４がＩＳＤＮ回線により接続されている場合は、ユーザーは２回線を独立に使用することができるので、前述の① のインターネット接続回線を切断することなく接続を維持したまま、もう一つの回線に対する電子決済認証システム５－３からのコールバックに対し電話端末５－４により応答し、その後の認証サービスを受けることができる。

【００５０】ユーザー端末５－１，５－４がアナログ電話回線により接続されている場合は、ユーザーは前述の① のインターネット接続を一旦切断し、電子決済認証システム５－３は該インターネット接続の切断を待って、ユーザーの電話端末５－４を呼び出す待ち合わせ呼出しを行う。

【００５１】アナログ電話回線のユーザーは電子決済認証システム５－３からの待ち合わせ呼出しに応答し、電話端末５－４からユーザーＩＤとクレジットカード番号を送信するが、その後の認証サービスは、インターネットを介した電子メールにより受けることとなる。

【００５２】また、ユーザー端末５－１，５－４が接続された回線がＩＳＤＮ回線である場合でも、前述したもう一つの回線が話中であったときは、電子決済認証システム５－３は前記① のインターネット接続の回線又はもう一つの回線の切断を待って、ユーザーの電話端末５－４をコールバックする待ち合わせ呼出しを行う。

【００５３】なお、ユーザーが通話中着信呼び出し（コールウェイティング）を受けられるサービスクラスである場合は、電子決済認証システム５－３は、前述の待ち合わせ呼出しの代わりに通話中着信呼び出しを行い、前述の① のインターネット接続回線を切断することなく維持したまま、電子決済認証システム５－３からのコールバックに応答し、その後の認証サービスを受ける構成とすることができる。

【００５４】次に図７の④ に示すように電子決済認証システム７－１は、専用線接続又はパケット交換網を介してクレジットカード決済システム７－２に、トランザクションＩＤ、ユーザーＩＤ、クレジットカード番号、商品名、個数等のデータを送信する。

【００５５】クレジットカード決済システム７－２は、図７の⑤ に示すようにサービスＩＤ、ユーザーＩＤ、認証結果等のデータを専用線接続又はパケット交換網を介

して電子決済認証システム７－１に送信する。

【００５６】次に図６の⑯に示すように電子決済認証システム６－２は、電子商取引サービスプロバイダのＷＷＷサーバー６－１に、トランザクションＩＤ、ユーザーＩＤ、認証結果、クレジットカード会社ＩＤ等のデータをインターネット接続を介して送信する。なお、これと同時に電子決済認証システム６－２（図５においては５－３）は、図５の⑯′に示すようにユーザーの電話端末５－４に公衆網を介して認証結果を音声によりアナウンスするようにしてもよい。

【００５７】最後に図５の⑰に示すように、電子商取引サービスプロバイダのＷＷＷサーバー５－２からインターネットを介してトランザクションＩＤとともに電子商取引の注文データの明細情報及び領収証を発行する。したがって、ユーザーは直ちにＷＷＷブラウザの画面上で電子商取引の認証結果を含む明細内容を確認することができる。

【００５８】次に図８及び図９とともに本発明の電子決済認証システム及び電子商取引サービスプロバイダ装置の動作フローを説明する。図８は本発明の電子商取引サービスプロバイダ装置の動作のフローチャートである。また図９は本発明の電子決済認証システムの動作のフローチャートである。

【００５９】電子商取引サービスプロバイダ装置は図８に示すステップ８－１において、インターネットの電子商取引サービスの開始状態となると、ステップ８－２において、ウェブサーバーにより商品購入支援画面を表示し、ステップ８－３において、ユーザーからのユーザーＩＤ、電話番号、希望商品名等の電子商取引の基本情報入力を待ち、該基本情報が入力されると、ステップ８－４において、電子決済認証システムに基本情報を送信する。

【００６０】電子決済認証システムは図９に示すステップ９－１において基本情報を受信すると、ステップ９－２において該ユーザーＩＤが加入者データベース記憶部に存在するか否かを調べ、存在すればステップ９－３において該ユーザーＩＤの電話番号を検索し、ステップ９－４において該ユーザーの回線はＩＳＤＮ回線かアナログ電話回線かを調べ、ＩＳＤＮ回線であればステップ９－５において登録電話番号によりコールバックする。

【００６１】また、ユーザーの回線がアナログ電話回線であればステップ９－６において話中の終了を待って呼び出す待ち合わせ呼び出し又は通話中着信（コールウェイティング）呼出しを行う。一方、ＩＳＤＮ回線のユーザーに対して前述のステップ９－５においてコールバックした際に、話中（ビジー）であったときは、ステップ９－６において同様に話中の終了を待って呼び出す待ち合わせ呼び出し又は通話中着信（コールウェイティング）呼出しを行う。

【００６２】ステップ９－７においてコールバックに対するユーザーの応答を検出すると、ステップ９－８において音声によるガイダンスをアナウンスし、ステップ９－９においてクレジットカード番号等の秘匿情報の入力を待つ。クレジットカード番号等の秘匿情報が入力されると、ステップ９－１０においてクレジットカード番号等の秘匿情報とトランザクションＩＤとをクレジットカード決済システム（クレジット会社）へ送信し、クレジットカード決済システムからその認証結果を受信する。

【００６３】クレジットカード決済システムから認証結果を受信すると、ステップ９－１１において、電子商取引サービスプロバイダ装置にトランザクションＩＤ及びクレジットカード番号の認証結果を送信する。なお、前述のステップ９－２においてユーザーＩＤが存在しなかった場合は、ステップ９－１２において受付内容を拒否するメッセージを生成し、ステップ９－１１によりそのメッセージを電子商取引サービスプロバイダ装置に送信する。

【００６４】電子商取引サービスプロバイダ装置が電子決済認証システムから認証結果を受信すると、図８に示すステップ８－５において認証結果の正常性を判定し、正常であればステップ８－６においてユーザー端末に対し、認証結果を示すクレジットカード認証済み及び領収証発行の画面表示とトランザクションＩＤの画面を表示して終了する。

【００６５】また、前述のステップ８－５の判定において認証結果が不正常であった場合は、ステップ８－７においてクレジットカード認証不可の画面を表示し、ステップ８－８において前述の開始ステップ８－１に戻る。

【００６６】図１０は本発明の電子商取引サービスの信号送受のシーケンスチャートである。同図において、ＬＳはユーザーを収容している加入者交換機、ＩＳＰはインターネットサービスプロバイダ、ＣＳＰは電子商取引サービスプロバイダである。

【００６７】ユーザーとインターネットサービスプロバイダ（ＩＳＰ）との間、及び電子決済認証システムを備えた認証センタとユーザーとの間は、加入者交換機（ＬＳ）を介し、公衆網であるＩＳＤＮ回線又はアナログ電話回線により接続される。

【００６８】インターネットサービスプロバイダ（ＩＳＰ）と電子商取引サービスプロバイダ（ＣＳＰ）との間はインターネットにより接続され、認証センタとクレジットカード決済システムを備えたクレジットカード会社との間は専用線又はパケット交換網により接続される。

【００６９】ユーザーは加入者交換機（ＬＳ）にインターネットサービスプロバイダ（ＩＳＰ）への呼を発し（１０－１）、ユーザーとインターネットサービスプロバイダ（ＩＳＰ）とが接続され（１０－２）、該ユーザーとインターネットサービスプロバイダ（ＩＳＰ）を経由してユーザーと電子商取引サービスプロバイダ（ＣＳＰ）とが接続される（１０－３）。

【００７０】ユーザーは、ユーザーＩＤ及び商品名等の商取引情報を電子商取引サービスプロバイダ（ＣＳＰ）に送信し（１０－４）、電子商取引サービスプロバイダ（ＣＳＰ）は、それらの情報を認証センタに送信する（１０－５）。

【００７１】認証センタはユーザーＩＤからユーザーの電話番号（ＴＥＬ＃）をデータベースにより調べ（１０－６）、電子商取引サービスプロバイダ（ＣＳＰ）にトランザクションＩＤを送信する（１０－７）。

【００７２】電子商取引サービスプロバイダ（ＣＳＰ）は該トランザクションＩＤをユーザーに送信し（１０－８）、また認証センタは加入者交換機（ＬＳ）に該ユーザーをコールバックするために発呼する（１０－９）。

【００７３】認証センタとユーザーとの間は公衆網を介して接続され（１０－１０）、認証センタはクレジットカード情報等の秘匿情報を入力するようにアナウンスを送出し（１０－１１）、ユーザーはトランザクションＩＤとユーザーＩＤとクレジットカード情報等の秘匿情報を電話端末により入力する（１０－１２）。

【００７４】認証センタは、電話端末により入力された秘匿情報をデータベースに一時的に登録し（１０－１３）、ユーザーとの間の公衆網を介した接続を切断する（１０－１４）。認証センタは更に電話端末により入力されたクレジットカード情報等の秘匿情報をクレジットカード会社に送信して問い合わせ（１０－１５）、クレジットカード会社は、該クレジットカード情報等の認証結果を認証センタに送信する（１０－１６）。

【００７５】認証センタは該認証結果を電子商取引サービスプロバイダ（ＣＳＰ）に送信し（１０－１７）、電子商取引サービスプロバイダ（ＣＳＰ）は該認証結果を基にクレジットカード認証済み確認証及び領収証をトランザクションＩＤとともに送信し（１０－１８）、ユーザーはそれを受けてログアウトし、インターネットサービスプロバイダ（ＩＳＰ）との接続の切断を要求する（１０－１９）。

【００７６】加入者交換機（ＬＳ）はユーザーからの切断要求により公衆網を介した接続を切断する（１０－２０）。電子商取引サービスプロバイダ（ＣＳＰ）は該電子商取引による商品代金をクレジットカード会社に請求し、クレジットカード会社はその代金をユーザーに請求することとなる。

【００７７】

【発明の効果】以上説明したように、本発明によれば、クレジットカード番号等の秘匿情報をユーザーから電子決済認証システムにのみ公衆網を介して直接送信し、該電子決済認証システムは該クレジットカード番号等の秘匿情報をクレジットカード決済システムに専用線等により直接問い合わせて一元的に集中管理することにより、クレジットカード情報等の秘匿情報がインターネット上で送受されず、秘匿情報の流出等に対する管理上の安全性を向上させることができ、また、ユーザーはクレジットカード情報等を各電子商取引サービスプロバイダに予め登録しておく必要がないため、簡便な操作により即時にオンラインショッピング等電子商取引サービスを利用することができる利点がある。

【００７８】更に、電子決済認証システムは、電子商取引サービス利用者をデータベース記憶部に記憶された加入者情報を基に呼び返すことにより本人の同定を行うため、電子商取引サービスプロバイダ及びユーザー側に、本人同定のための特別な認証装置を必要せず、簡易な構成により本人の同定を行うことができ、ユーザーの不当行為等による料金の不正請求等のトラブル発生を防ぐことができる。

【００７９】電子商取引サービスプロバイダ装置は、電子決済認証システムからユーザーのクレジットカードの有効性が通知されるため、ユーザーのクレジットカード情報の保持、管理を行う必要がなく、簡易にシステムを構成することができる。

【００８０】ユーザーと電子商取引サービスプロバイダとの間で交わされた電子商取引に関するトランザクションデータを、電子決済認証システムにおいて識別子を付して管理することにより、電子商取引情報及び秘匿情報の送受信の一連の通信データを、該電子決済認証システムにおいて一元的に管理することができ、誤請求等のトラブルの発生時の確認作業が容易となり、電子商取引サービス信頼性を向上させることができる。

【図面の簡単な説明】

【図１】本発明の電子商取引サービスシステムの説明図である。

【図２】本発明の電子決済認証システムの主要部を示す図である。

【図３】本発明の電子決済認証システムの機能ブロック図である。

【図４】本発明の電子決済認証システムのデータベース記憶部の内容を示す図である。

【図５】本発明の電子商取引サービスの通信手順の説明図である。

【図６】本発明の電子商取引サービスの通信手順の説明図である。

【図７】本発明の電子商取引サービスの通信手順の説明図である。

【図８】本発明の電子商取引サービスプロバイダ装置の動作のフローチャートである。

【図９】本発明の電子決済認証システムの動作のフローチャートである。

【図１０】本発明の電子商取引サービスの信号送受のシーケンスチャートである。

【符号の説明】

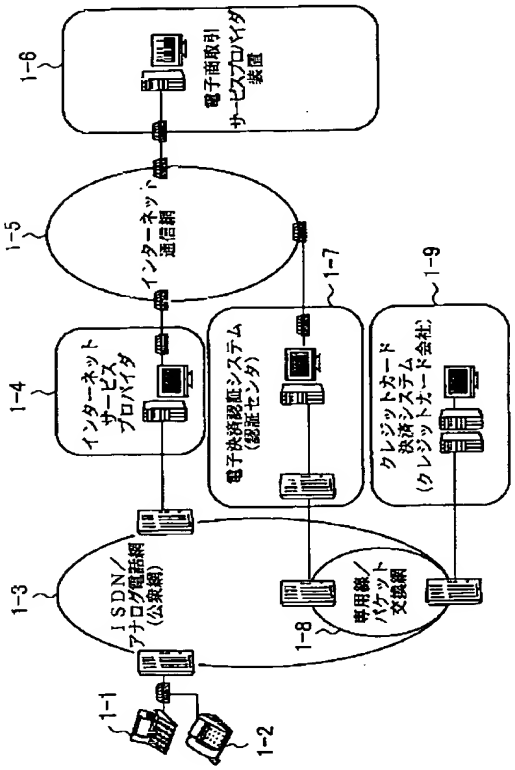
１－１　ユーザーの情報機器端末

１－２　同ユーザーの電話端末

1－3　ＩＳＤＮ又はアナログ電話網
1－4　インターネットサービスプロバイダ装置
1－5　インターネット通信網
1－6　電子商取引サービスプロバイダ装置
1－7　電子決済認証システム
1－8　専用線又はパケット交換網
1－9　クレジットカード決済システム

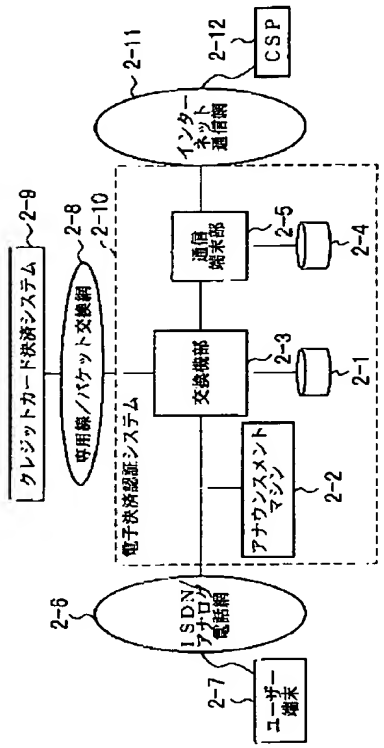
【図１】

本発明の電子商取引サービスシステムの説明図



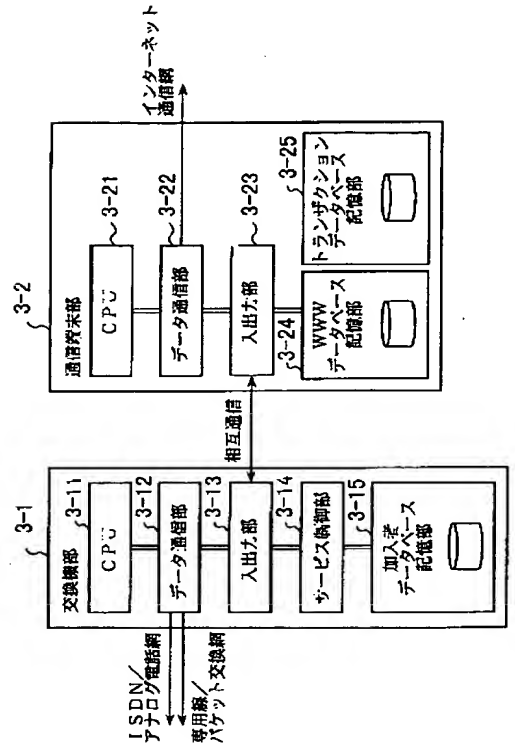
【図２】

本発明の電子決済認証システムの主要部を示す図



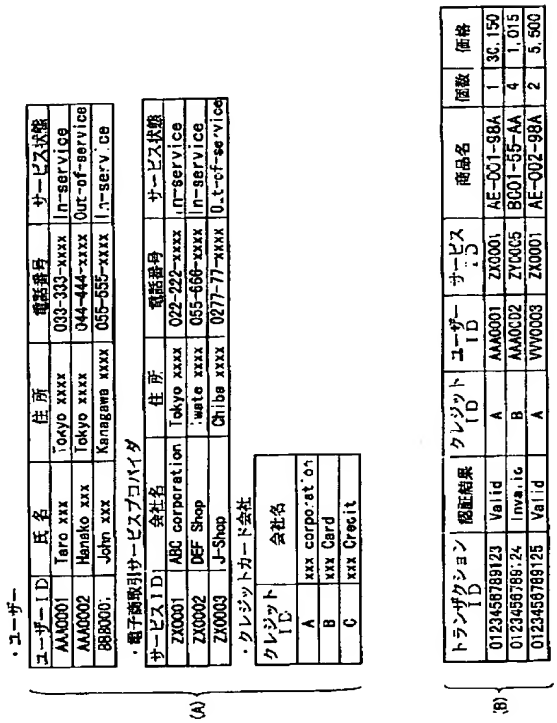
【図3】

本発明の電子決済認証システムの機能ブロック図



【図4】

本発明の電子決済認証システムのデータベース記憶部の内容を示す図



・ユーザー

ユーザーID	氏名	住所	電話番号	サービス状態
AAA0001	Taro xxx	Tokyo xxxx	033-333-xxxx	In-service
AAA0002	Hanako xxx	Tokyo xxxx	044-444-xxxx	Out-of-service
888000:	John xxx	Kanagawa xxxx	055-555-xxxx	In-service

・電子商取引サービスプロバイダ

サービスID	会社名	住所	電話番号	サービス状態
ZX0001	ABC corporation	Tokyo xxxx	022-222-xxxx	In-service
ZX0002	DEF Shop	Iwate xxxx	055-666-xxxx	In-service
ZX0003	J-Shop	Chiba xxxx	0277-77-xxxx	Out-of-service

・クレジットカード会社

クレジットID	会社名
A	xxx corporation
B	xxx Card
C	xxx Credit

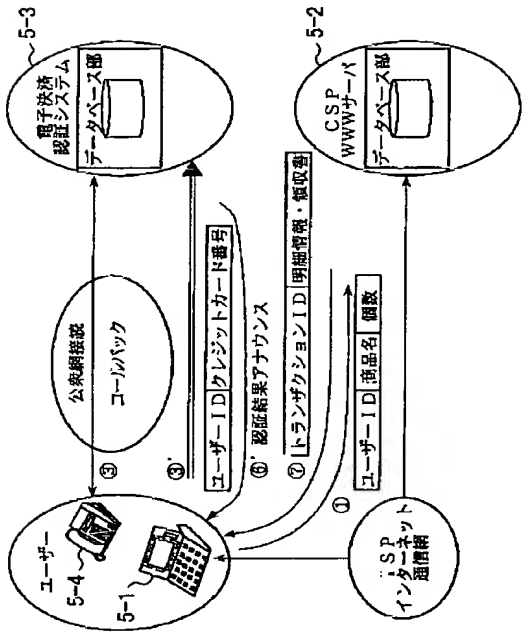
(A)

トランザクションID	認証結果	クレジットID	ユーザーID	サービスID	商品名	個数	価格
0123456789123	Valid	A	AAA0001	ZX0001	AE-001-98A	1	30,150
0123456789124	Invalid	B	AAA0002	ZX0005	B001-55-AA	4	1,015
0123456789125	Valid	A	WW0003	ZX0001	AE-002-98A	2	5,500

(B)

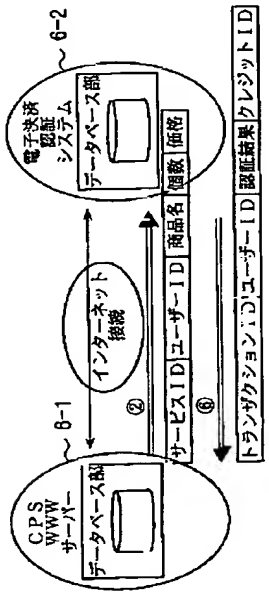
【図5】

本発明の電子商取引サービスの通信手順の説明図



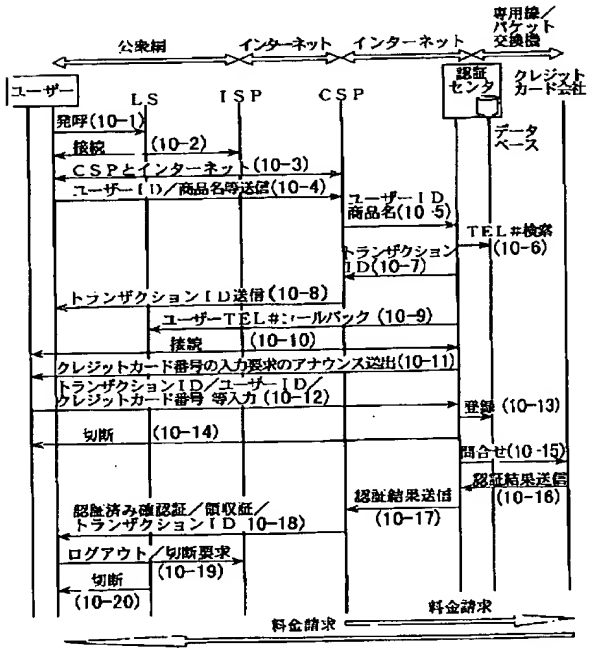
【図6】

本発明の電子商取引サービスの通信手順の説明図



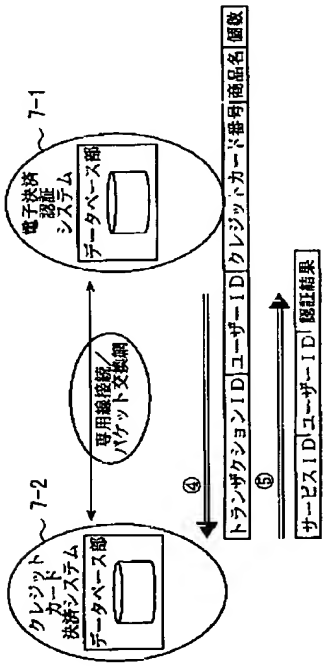
【図10】

本発明の電子取引サービスの信号受信のシ･-ケンスチャート



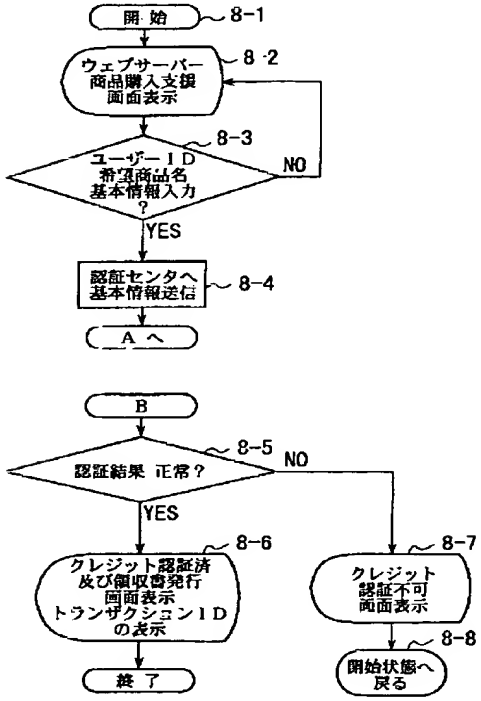
【図7】

本発明の電子商取引サービスの通信手順の説明図



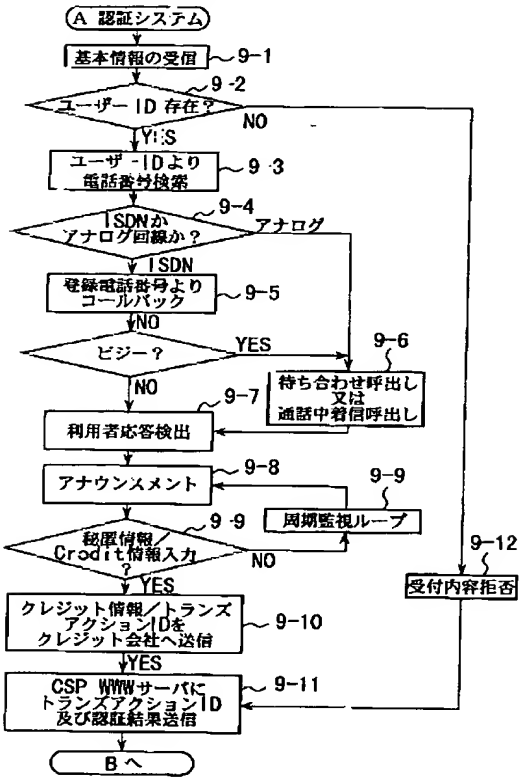
【図8】

本発明の電子商取引サービスプロバイダ装置の動作のフローチャート



【図９】

本発明の電子決済認証システムの動作のフローチャート



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		(参考)
Ｈ０４Ｍ　3/42		Ｈ０４Ｌ　11/20	１０１Ｚ	